Política de Segurança das Informações e Segurança Cibernética

Rio de Janeiro, 12 de fevereiro 2019

I – SISTEMA DE SEGURANÇA DAS INFORMAÇÕES

1.1. Caracterizam o Sistema de Segurança das Informações da AGUILA CAPITAL:

(i) Monitoramento de todas as estações trabalho, da retirada não autorizada de arquivos por meio digital da empresa, de acesso aos conteúdos online, restrição a instalação de programas não autorizados, monitoramentos do envio e recebimento de e-mails;

(ii) Gravação e controle do áudio de todas as ligações originadas ou recebidas pelos sistemas de telefonia da AGUILA CAPITAL;

(iii) Armazenagem física de documentos relevantes para a AGUILA CAPITAL pelo tempo requerido por lei, de forma própria ou por terceiros contratados para este fim;

(iv) Destruição de documentos descartados, de forma a garantir que informações relevantes não sejam repassadas à terceiros;

(v) Realização de procedimentos de backup dos sistemas de informação e dados digitais de forma compatível com as necessidades da empresa.

1.2. Nenhuma informação confidencial deve, em qualquer hipótese, ser divulgada a pessoas, dentro ou fora da AGUILA CAPITAL, que não necessitem de, ou não devam ter acesso a tais informações para desempenho de suas atividades profissionais.

1.3. Qualquer informação sobre a AGUILA CAPITAL, ou de qualquer natureza relativa às atividades da AGUILA CAPITAL, aos seus sócios e clientes, obtida em decorrência do desempenho das atividades normais do Colaborador na AGUILA CAPITAL, só poderá ser fornecida ao público, mídia ou a demais órgãos caso autorizado por escrito pelo *Compliance Officer*.

1.4. É terminantemente proibido que os Colaboradores façam cópias ou imprimam os arquivos utilizados, gerados ou disponíveis na rede da AGUILA CAPITAL e circulem em ambientes externos à AGUILA CAPITAL com estes arquivos, uma vez que tais arquivos contêm informações que são consideradas informações confidenciais.

1.5. A proibição acima referida não se aplica quando as cópias ou a impressão dos arquivos forem em prol da execução e do desenvolvimento dos negócios e dos interesses da AGUILA CAPITAL e de seus clientes. Nestes casos, o Colaborador que estiver na posse e guarda da cópia ou da impressão do arquivo que contenha a informação confidencial será o responsável direto por sua boa conservação, integridade e manutenção de sua confidencialidade.

1.6. Ainda, qualquer impressão de documentos deve ser imediatamente retirada da máquina impressora, pois podem conter informações restritas e confidenciais, mesmo no ambiente interno da AGUILA CAPITAL.

1.7. O descarte de informações confidenciais em meio digital deve ser feito de forma a impossibilitar sua recuperação. Todos os arquivos digitalizados em pastas temporárias serão apagados periodicamente, de modo que nenhum arquivo deverá ali permanecer. A desobediência a esta regra será considerada uma infração, sendo tratada de maneira análoga à daquele que esquece material na área de impressão.

1.8. O descarte de documentos físicos que contenham informações confidenciais ou de suas cópias deverá ser realizado imediatamente após seu uso, de maneira a evitar sua recuperação.

1.9. A utilização de mídia removível (tais como pen-drives, discos flexíveis, cartões de memória e similares) ficará vedada e os dispositivos desabilitados. Exceções à política serão analisadas pelo *Compliance Officer*.

1.10. É proibida a conexão de equipamentos na rede da AGUILA CAPITAL que não estejam previamente autorizados pela área de informática e pela área de *compliance*.

1.11. Cada Colaborador é responsável por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos que estão sob sua responsabilidade.

1.12. O envio ou repasse por e-mail de material que contenha conteúdo discriminatório, preconceituoso, obsceno, pornográfico ou ofensivo é também terminantemente proibido, conforme acima aventado, bem como o envio ou repasse de e-mails com opiniões, comentários ou mensagens que possam denegrir a imagem e/ou afetar a reputação da AGUILA CAPITAL.

1.13. Em nenhuma hipótese um Colaborador pode emitir opinião por e-mail em nome da AGUILA CAPITAL, ou utilizar material, marca e logotipos da AGUILA CAPITAL para assuntos não corporativos ou após o rompimento do seu vínculo com este, salvo se expressamente autorizado para tanto.

1.14. O *Compliance Officer* também monitorará os diretórios e *logins* virtuais no servidor protegidos por senha. O *Compliance Officer* elucidará as circunstâncias da ocorrência deste fato e aplicará as devidas sanções.

Programas instalados nos computadores, principalmente via internet (downloads), sejam de utilização profissional ou para fins pessoais, devem obter autorização prévia do responsável pela área de informática na AGUILA CAPITAL. Não é permitida a instalação de nenhum software ilegal ou que possua direitos autorais protegidos. A instalação de novos softwares, com a respectiva licença, deve também ser comunicada previamente ao responsável pela informática. Este deverá aprovar ou vetar a instalação e utilização dos softwares dos Colaboradores para aspectos profissionais e pessoais.

1.15. A AGUILA CAPITAL se reserva no direito de implementar se necessário a gravação de qualquer ligação telefônica e/ou qualquer comunicação dos seus Colaboradores realizada ou recebida por meio das linhas telefônicas ou qualquer outro meio disponibilizado pela AGUILA CAPITAL para a atividade profissional de cada Colaborador. O *Compliance Officer* é encarregado de, regularmente, monitorar, por amostragem, as ligações e demais comunicações realizadas pelos Colaboradores. Qualquer informação suspeita encontrada será esclarecida imediatamente pelo *Compliance Officer* com registro em ata.

1.16. Todas as informações do servidor da AGUILA CAPITAL, do banco de dados dos clientes e os modelos dos analistas são enviados para o servidor interno. Nesse servidor, as informações são segregadas por área e transformadas em pacotes criptografados, sendo armazenadas com backup.

II - POLÍTICA DE SEGURANÇA CIBERNÉTICA

2.1. A segurança cibernética é o conjunto de tecnologias, processos e práticas projetados para proteger a rede, os computadores, os sistemas e os dados de ataques ou acessos não autorizados.

2.2. O risco de ataque cibernético ameaça os princípios da segurança das informações, tais como confidencialidade, integridade e disponibilidade.

2.3. Há diversas razões para que esses ataques ocorram e os principais motivos são:

(i) obter recursos financeiros;

(ii) roubar e manipular informações;

(iii) obter informações privilegiadas;

(iv) sabotagem à instituição;

(v) disseminar falsas notícias; e

(vi) disseminar o caos.

A segurança cibernética deve garantir:

(i) a segurança dos sistemas e dos bancos de dados;

(ii) o gerenciamento das pessoas autorizadas;

(iii) a segurança dos sistemas e informações que estão na nuvem;

(iv) a segurança para todos os dispositivos/equipamentos;

(v) o planejamento da continuidade do negócio; e

(vi) o treinamento constante do usuário final, com o objetivo de minimizar a vulnerabilidade da organização.

2.4. São exemplos de consequências/danos que podem ser causados pela falha na segurança cibernética:

(i) risco de imagem;

(ii) risco de continuidade do negócio; e

(iii) prejuízos financeiros.

2.5. A empresa prestadora de serviços de TI é a responsável pelo mapeamento dos riscos internos e externos, dos equipamentos e softwares utilizados pela AGUILA CAPITAL.

2.6. O *Compliance Officer* é responsável pela análise dos riscos mapeados e pela implantação/investimento dos processos que precisam de proteção e monitoramento.

2.7. Todo o procedimento operacional é monitorado por empresa prestadora de serviços de TI, especializada em TI.

2.8. A empresa prestadora de serviços de TI é a responsável pelo monitoramento e emite relatórios semanais e mensais que medem a disponibilidade dos servidores e das estações de trabalho contendo a relação das atualizações realizadas e possíveis pontos de vulnerabilidades, serviços do Windows e atualizações dos antivírus.

2.9. A capacidade e efetividade do plano de resposta é vital para proteger as informações e os recursos de informação da AGUILA CAPITAL, clientes e usuários.

2.10. Todo o procedimento operacional é monitorado. Os recursos de TI são monitorados por sistemas automatizados que fornecem informações atualizadas sobre a indisponibilidade dos serviços com registro de incidentes para providências e encaminhamento de soluções e está preparada para possibilitar um plano de resposta de forma ágil e consistente.

2.11. Caso a AGUILA CAPITAL sofra algum ataque cibernético que ocasione a perda de acesso aos sistemas, os responsáveis por cada área estão autorizados a acionar a equipe de help desk da empresa prestadora de serviços de TI e ativar os acessos aos sistemas de back-up em nuvem da AGUILA CAPITAL, de forma que todo o trabalho operacional possa ser mantido.

III - REVISÃO

Esta Política de Segurança das Informações e de Segurança Cibernética será revisada, no mínimo, anualmente pelo *Compliance Officer*. Serão utilizadas como base para a sua atualização as legislações, instruções, e regulamentações e autorregulamentações vigentes na data da sua revisão e estará vigente e aplicável mesmo durante o período de licenças/ausências dos membros na AGUILA CAPITAL.

IV - SANÇÕES

Esta Política de Segurança das Informações e de Segurança Cibernética se aplica a todos os usuários da rede corporativa da AGUILA CAPITAL, a quem caberá o atendimento às diretrizes e procedimentos ora estabelecidos, de forma a informar à Diretoria de Compliance sempre que se presenciar o seu descumprimento.

São exemplos que podem ocasionar em sanções:

(i) uso ilegal de software;

(ii) introdução intencional de vírus;

(iii) acesso a dados e sistemas não autorizados; e

(iv) divulgação de informações confidenciais.

Os colaboradores que violarem essa Política estarão sujeitos aos cumprimentos de determinadas sanções, tais como:

(i) responsabilidade civil por perdas e danos provocados aos fundos e/ou clientes da AGUILA CAPITAL;

(ii) ação disciplinar por parte dos agentes reguladores e autorreguladores, incluindo a revogação de autorização e multas;

(iii) responsabilidade criminal; e

(iv) advertência verbal, advertência escrita ou rescisão contratual, conforme a gravidade do caso.